

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/831,046	05/03/2001	Martin Euchner	P01,0142	8224
24131	7590	08/09/2004	EXAMINER	
LERNER AND GREENBERG, PA P O BOX 2480 HOLLYWOOD, FL 33022-2480			DINH, MINH	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 08/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/831,046

Applicant(s)

EUCHNER, MARTIN

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5/3/2001.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

Art Unit: 2132

DETAILED ACTION

1. Claims 1-10 have been examined.

Oath/Declaration

2. The oath or declaration is defective. The title of the invention identified in the declaration does not match the title identified in the specification.

Specification

3. The disclosure is objected to because of the following informalities:
 - a. The group of units Z_n^* with n as a composite integer (par. 0021) is in a separate category and does not belong to the multiplicative group F_q^* of a finite body F_q (paragraphs 0017-0020).
 - b. The phrase " $gx \bmod p$ " (substitute specification, par. 0044) should be changed to " $g^x \bmod p$ " (see figures 1 and 2).

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-3 and 7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2132

- a. Regarding claim 1, it recites the limitation "a second code" in the 8th line. There is no reference to a first code. For examination purpose, the limitation is interpreted as "a code"
- b. Regarding claim 1, it recites the limitation "said second key" in the 14th line. There is insufficient antecedent basis for this limitation in the claim. For examination purpose, the limitation is interpreted as "a second key".
- c. Regarding claim 2, it recites the limitation "and said first operation is an RSA function xg ". The first function is either a Diffie-Hellman function or an RSA function (specification, par. 0016). The limitation is interpreted as "or said first operation is an RSA function xg ".
- d. Regarding claim 3, the limitation "a group of units Z_n^* with n as a composite integer (8th line) does not belong to the multiplicative group F_q^* of a finite body F_q (3rd line). For examination purpose, the limitation is treated as a separate category.
- e. Regarding claim 7, it recites the limitation "said transmitted data". There is insufficient antecedent basis for this limitation in the claim. For examination purpose, the limitation is interpreted as "transmitted data".

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2132

7. Claims 1-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Jablon ("Strong Password-Only Authenticated Key Exchange").

a. Regarding claim 1, which is representative of claims 8 and 10, Jablon discloses a method, comprising the steps of:

carrying out a first operation $A(R_A, g)$ on a prescribed known value g and on a value R_A known only to a first entity, which meets the limitation of x , said first operation $A(R_A, g)$ being an asymmetric cryptographic method, thus producing a first operation result (Section 3.2 DH-EKE, p. 5);

encoding said first operation result utilizing a first key, which is a password and known to said first and to a second entity, said encoding being carried out with said first key utilizing a symmetrical encoding method, thus producing an encoded first operation result, said first operation result being a code with which said first entity is authorized to undertake a service on said second entity (Section 3.2 DH-EKE, p. 5; Section 3, p. 4, 3rd and 5th paragraphs);

transmitting said encoded first operation result by said first entity to said second entity (Section 3.2 DH-EKE, p. 5);

decoding said encoded first operation result by said second entity with said first key, and the first entity is thereby authenticated (Section 3.2 DH-EKE, p. 5; Section 3, p. 4, 3rd and 5th paragraphs);

Art Unit: 2132

determining a second key in relation to $G(gR_A R_B)$, by said second entity carrying out a second operation $G(gR_B)$ with a secret number R_B known only to it, which meets the limitation of y (Section 3.2 DH-EKE, p. 5);

encoding a result of said second operation with said first key (Section 3.2 DH-EKE, p. 5); and

transmitting said encoded second operation result to said first entity (Section 3.2 DH-EKE, p. 5).

b. Regarding claim 2, Jablon further discloses that the first operation is a Diffie-Hellman function ($G(\alpha R_A)$), $G()$ being an arbitrary, finite cyclic group G (Section 3.2 DH-EKE, p. 5; Section 3, p. 4, 4th paragraph).

c. Regarding claim 3, Jablon further discloses that the first operation is carried out in the multiplicative group \mathbf{Z}_p^* of the integers modulo prime p (Appendix A, p. 22, 1st paragraph.).

d. Regarding claim 4, Jablon further discloses that the second key is a session key (Section 3.2 DH-EKE, p. 5; Section 3, p. 4, 5th paragraph).

e. Regarding claim 5, Jablon further discloses that the Diffie-Hellman method is used to generate the second key (Section 3.2 DH-EKE, p. 5).

f. Regarding claims 6 and 9, Jablon further discloses encoding being carried out with the first key utilizing a cryptographic one-way function (Section 1.1, p. 2, 7th paragraph).

g. Regarding claim 7, Jablon further discloses that transmitted data are confidential data. (Section 3.2 DH-EKE, p. 5; Section 3, p. 4, 2nd and 3rd paragraphs).

Art Unit: 2132

Conclusion


8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Menezes, "Handbook of Applied Cryptography", discloses the discrete logarithm problem.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

MD
Minh Dinh
Examiner

Application/Control Number: 09/831,046

Page 7

Art Unit: 2132

Art Unit 2132

MD

7/28/04